EXHIBIT N

Al-Naji, Chen, Diao, Basis Whitepaper

EXHIBIT N

Basis: A Price-Stable Cryptocurrency with an Algorithmic Central Bank

Formerly known as: Basecoin

Nader Al-Naji (n@intangiblelabs.co), Josh Chen (j@intangiblelabs.co), Lawrence Diao (l@intangiblelabs.co)

Version 0.99.7
First published: June 20, 2017
Last updated: June 4, 2018

For the most updated version, see:
www.basis.io

Contents

Abstract **1**

Introduction: Why Does Price Stability Matter? **1**

Use Cases for a Price-Stable Cryptocurrency **3**
Developing Markets . . . 3
A Low-Volatility Cryptoasset for Traders . . . 5
Credit and Debt Markets . . . 6
The Broader Blockchain Economy . . . 7
Fighting Macroeconomic Depressions . . . 7

How Basis Implements Price Stability **8**
The Quantity Theory of Money . . . 9
The Basis Protocol . . . 10
Measuring the Exchange Rate . . . 11
Expansion and Contraction via a Three-Token System . . . 13
A Few Technical Notes . . . 16
Robustness . . . 16
Price Responsiveness . . . 17

A Post-USD World **18**
Stabilizing to a CPI . . . 18
A Regional Basis for Each Regional Economy . . . 19

Other Attempts at a Stable Coin **20**
Seigniorage Shares . . . 20
MakerDAO . . . 21
Tether . . . 23
BitShares . . . 23

Conclusion **25**

Contact **25**

Abstract

The price volatility of Bitcoin and other cryptocurrencies is one of the biggest barriers to widespread adoption that cryptocurrencies face today. Unlike fiat currencies, today's cryptocurrencies do not have a central bank that implements monetary policy to keep purchasing power stable, meaning that changes in demand can induce massive fluctuations in price. If users cannot be sure that the purchasing power of their accounts will remain stable, they will never adopt a cryptocurrency as a medium of exchange over a price-stable alternative. Moreover, without price stability, it is difficult for credit and debt markets to form on top of a cryptocurrency because every contract taking payments in the future must charge a large premium to factor in price risk. For example, imagine you received a salary of 1 BTC per month—if the price of BTC dropped, you might miss rent.

While much cryptocurrency research has been dedicated to technical topics such as transaction throughput and smart contracts, almost no attention in comparison has been paid to improving price stability, a problem we believe to be a much bigger obstacle to the mass adoption of cryptocurrencies as a medium of exchange. In this paper, we introduce Basis, a cryptocurrency whose tokens can be robustly pegged to arbitrary assets or baskets of goods while remaining completely decentralized. For example, to start off, 1 Basis can be pegged to always trade for 1 USD. In the future, Basis could potentially even eclipse the dollar and be updated to peg to a consumer price index (CPI) or basket of goods, similar to how central banks hit inflation targets today. The Basis protocol accomplishes this by algorithmically adjusting the supply of Basis tokens in response to changes in, for example, the Basis-USD exchange rate. This implements a monetary policy similar to that executed by central banks around the world, except it operates as a decentralized, protocol-enforced algorithm, without the need for direct human judgment. For this reason, Basis can be understood as implementing an algorithmic central bank.

Introduction: Why Does Price Stability Matter?

Today, very few people use cryptocurrencies for normal, day-to-day transactions. But why?

Some would say it's because cryptocurrencies are slow and expensive to use. While that's true of Bitcoin and many older cryptocurrencies, it's certainly not true of some newer protocols. For example, Dash claims it can confirm transactions in under a second and handle thousands of transactions per second at fees of less than $0.15 per

transaction, with fees expected to decrease further over time. Others would say it's because cryptocurrencies aren't reliable or trusted. But that's also not true, as there are many protocols with firm backing from respected investors and strong development teams. Furthermore, Bitcoin itself has shown that the blockchain model is extremely robust from a fault-tolerance perspective.

Some would say cryptocurrencies aren't widely used because there is an inherent chicken and egg problem: Because everyone uses local currency, merchants don't have an incentive to accept anything else. But we actually think the opposite is true. As long as some customers want to pay in cryptocurrency, it costs merchants almost no overhead to accept it, and it costs them sales if they don't. In fact, because cryptocurrencies are immune to fraudulent chargebacks, and transaction fees can be much lower than fees for credit and even debit cards, merchants should actually prefer cryptocurrency payments.

We can find two clues to the real problem by examining the perspectives of the merchant and the customer in turn. First, consider the merchants that do accept cryptocurrency payments today. Microsoft, Quickbooks, and Spotify, for example, allow customers to pay in Bitcoin using a service called BitPay. However, none of these merchants keep their money in Bitcoin—instead, they immediately convert any Bitcoin they receive into USD. Why? Well, these merchants are not in the business of speculating on Bitcoin. They don't want exposure to Bitcoin market risk any more than they want to hold their money in barrels of oil. What if Bitcoin dropped 90% one day? If you ask people who love cryptocurrencies, they might mention many of the attributes they love—for example, the convenience, the control, and the semi-anonymity. But we bet they still can't stomach the idea of keeping their life savings or quarterly revenue invested in such a volatile asset. In other words, in order for cryptocurrencies to become more than just a playground for speculation, there is a severe need for them to be a stable store of value.

Second, imagine trying to make a purchase using Bitcoin. Because merchants want to collect a fixed amount of USD for their services, you're faced with a constantly adjusting BTC price for your potential purchase. This is a terrible user experience. Even worse, imagine receiving a job offer that pays 1 BTC per month. If the price of BTC happened to drop one month, you can't pay your bills. Alternatively, if you borrowed money via a loan that demands a monthly payment of 1 BTC, a price swing in the other direction could leave you in default. We'll discuss this more later, but the fundamental problem is that today's price-volatile cryptocurrencies subject any contract promising or taking future payments to extreme price risk. From this, we can see that in order for cryptocurrencies to become a viable medium of exchange or unit of account, there is again a severe need for price stability.

Any currency has three fundamental functions: A store of value, a medium of exchange, and a unit of account. We believe that price stability is a gatekeeper to the mainstream adoption of a currency for any of these purposes. In this whitepaper, we introduce Basis, the first cryptocurrency to implement robust, decentralized, and protocol-enforced price stability. Specifically, we discuss the following topics:

- Use Cases for a Price-Stable Cryptocurrency: A number of valuable use cases in which a price-stable cryptocurrency would be preferred over the best alternative today.
- How Basis Implements Price Stability: A specification of a fully-decentralized, price-stable cryptocurrency protocol, and why it is robust.
- A Post-USD World: How a world economy denominated in Basis looks.
- Other Attempts at a Stable Coin: Why other attempts at developing a stable coin are insufficiently robust.

Use Cases for a Price-Stable Cryptocurrency

Developing Markets

People living in developed economies take for granted their access to stable currencies. If you're in the US with unfettered access to dollars, or in the EU with access to euros, you may wonder why the world needs a price-stable cryptocurrency. However, in countries with weak institutions and unstable currencies, high rates of inflation and currency devaluation are common. In these markets, we expect a price-stable cryptocurrency will be in high demand.

As of publication in Q3 2017, Egypt is suffering 32% annual inflation, Argentina 23%, and Nigeria 16%. And this is just a sampling of countries whose governments are relatively more stable—let's not forget Venezuela, whose annual inflation rate is currently at 741%. What would you do if your savings were disappearing at a rate of 741% a year? Faced with a rapidly devaluing local currency, people look for other ways to survive, frequently flocking to the USD. This effect is known as dollarization. Generally, it takes three forms:

- First, a population might choose to adopt the dollar over local currency without any coordination from the local government. The USD is used as the de facto currency in a number of Central Asian and sub-Saharan African countries, and the rate of adoption can be overwhelmingly fast despite the lack of official coordination. For example, in the 2 years from 2006 to 2008, dollarization in

the Seychelles jumped from 20% to 60%.

- Second, a country's citizens might demand the dollar in spite of government capital controls that prevent the transfer of USD across its borders. Argentina's black market for dollars, the *dolar blue*, was an open secret during its reign of capital controls from 2011 to 2015. During these years, $10 million to $40 million per day changed hands under the table at rates that were 25-30% above the official exchange rate. These rates were even published daily in national newspapers, despite it being officially illegal.
- Third, currency devaluation could grow so extreme that governments might officially switch to the USD, as happened in Zimbabwe in 2009. Today, the entire country requires routine shipments of physical paper dollars and coins.

Isn't there an opportunity here? Whether or not dollarization is officially endorsed, citizens, banks, and governments incur significant costs in importing physical USD. **A cryptocurrency solution, by which millions of dollars could be transported on one's phone, seems like a vastly superior alternative to paper dollars in all dollarization scenarios.**

As a final aside: Existing cryptocurrencies have found some traction off in some hyperinflating economies—for example, Bitcoin usage has been growing in Venezuela as it has faced its currency crisis. However, Bitcoin can never truly free people from their unstable local currencies due to its own lack of price stability. For example, if Bitcoin is going through a cycle of devaluation, users perceive no difference between it and a devaluing local currency. Even if Bitcoin crashes just once, people will want to move to a price-stable alternative—should one exist. A stable coin would thus be the killer app for developing economies experiencing rapid currency devaluation. In the extreme case, instead of switching to importing paper dollars and coins, the next country to switch away from its local currency like Zimbabwe did could instead adopt a price-stable cryptocurrency.

Along these lines, in a 2017 speech, the Managing Director of the International Monetary Fund, Christine LaGarde, proposed:

> [T]hink of countries with weak institutions and unstable national currencies. Instead of adopting the currency of another country—such as the U.S. dollar—some of these economies might see a growing use of virtual currencies. Call it dollarization 2.0.
>
> IMF experience shows that there is a tipping point beyond which coordination around a new currency is exponential. In the Seychelles, for example, dollarization jumped from 20 percent in 2006 to 60 percent in 2008.
>
> And yet, why might citizens hold virtual currencies rather than physical

> dollars, euros, or sterling? Because it may one day be easier and safer than obtaining paper bills, especially in remote regions. And because virtual currencies could actually become more stable.
>
> For instance, they could be issued one-for-one for dollars, or a stable basket of currencies. Issuance could be fully transparent, governed by a credible, pre-defined rule, an algorithm that can be monitored. . . or even a "smart rule" that might reflect changing macroeconomic circumstances.
>
> So in many ways, virtual currencies might just give existing currencies and monetary policy a run for their money.

A Low-Volatility Cryptoasset for Traders

Today, many traders on cryptocurrency exchanges convert their cryptocurrency into USD when there's turbulence in the crypto markets. But this is problematic for a few reasons.

First, some of the top crypto exchanges in the world are crypto-only, meaning they don't support conversions into fiat currencies. On such exchanges, traders are in desperate need of a price-stable cryptocurrency that they can use to wait out dips in the broader crypto market. To fill this need, a centralized solution known as USD Tether has arisen—but, for reasons discussed later, a centralized solution like Tether is unlikely to work in the long term, and Tether has faced significant negative sentiment as a result. To that end, Tether's $2.2 billion market cap proves the need, but it is also incapable of serving it long term.

Additionally, exchanges often list their trading pairs against some base currency. To trade these pairs effectively, users must hold some amount of that base currency, and they must also understand and evaluate prices as defined in that base currency. If this base currency were a volatile asset like Bitcoin, people would have to hedge any Bitcoin exposure they didn't want and constantly convert the price of the trading pair to their local unit of account. Most traders who don't have access to automated trading tools have a difficult time hedging or making conversions, and exchanges catering to a wider audience have a strong need for a stable cryptoasset like Basis.

Only a price-stable cryptocurrency can fulfill these needs of cryptocurrency traders. **Because cryptocurrency traders are naturally already enthusiastic about new protocols, this is also where we expect the initial demand for Basis to come from (i.e., the "early adopters").**

Credit and Debt Markets

Because of their volatility, today's cryptocurrencies are unsuitable for even the most basic financial contracts that our economy relies on. Can you imagine taking a job that pays 1 Bitcoin a month, but still paying your monthly bills in USD—what would happen to you and your family if the price of BTC crashed? What about buying a house with a 30-year mortgage denominated in Bitcoin, but living in a world in which you're probably still paid in dollars? These hypotheticals are unfathomable because credit and debt markets, and in fact markets for any financial contract over time, depend on price stability.

As a lender, when you structure a mortgage contract, the biggest risk that you take on is typically the risk of default. But if that mortgage were denominated in a volatile asset like Bitcoin, you're also exposed to extreme price risk. For example, a 30-year home loan denominated in Bitcoin is suddenly worth very little if the price of Bitcoin dropped 90% any day in the next 30 years. To sign the deal, you must either be willing to speculate on the price of Bitcoin in every loan you make, or you must find a speculator who is. Either way, you end up charging the borrower a premium for you or a speculator's willingness to hedge price risk. This adds substantial friction to the simplest of financial contracts.

By definition, this friction simply doesn't exist in a price-stable currency. Stable currencies thus reduce costs and increase liquidity for all sorts of financial instruments. At a deeper level, to maintain their stable price, price-stable currencies still require speculators who are willing to trade on expansions and contractions of the money supply. However, instead of operating on individual contracts, speculators operate on the currency itself, creating a pre-hedged, price-stable fungible asset that can be used to structure any deal as a derivative. This is like going from a world in which every home must have its own power generator, to a world in which a power plant leverages economies of scale and generates electricity for whole cities.

As cryptocurrency usage increases, we expect that demand will rise for a cryptocurrency usable for salaries, loans, bets, futures, options contracts, and more. In a price-volatile cryptocurrency, all contracts that involve payments through time require the friction of a speculator. **On the other hand, by offering price stability, Basis is unique in enabling capital markets to form directly on top of its protocol. This is a source of demand that we expect will grow larger and larger as time goes on.**

The Broader Blockchain Economy

A number of visionaries in the blockchain industry believe that we will soon see an ecosystem of "blockchain apps" arise, reimplementing existing services in a decentralized manner. For example, we may one day see a "blockchain Uber" or "blockchain Airbnb," each with its own app token. In fact, this is already happening with Filecoin reimplementing the Internet's storage layer. See this blog post for a great description of what this broader blockchain economy might look like.

Of course, if each blockchain app were to create its own token, there will need to be an interchange system to convert between some "universal token" and all of the different app tokens. We expect that everyone will hold this universal token and pay with it when using a blockchain app. Then, upon payment, the universal token will immediately get converted into the app token at the market rate. This would be similar to having your bank account in USD and using your debit card in a foreign country like Spain, in which case your bank converts your USD into EUR at the market rate every time you make a purchase, without you having to think about it.

If this ecosystem of blockchain apps arose, necessitating the need for a universal token, it would be very strange if that universal token were not price-stable. For example, imagine if your daily bus ride to work required $5 today and $50 tomorrow. Even more importantly, as we'll elaborate on in the next section, a price-volatile coin is vulnerable to hoarding incentives. If people believe that a coin will appreciate in the future, they are incentivized not to spend their precious appreciating assets. This would kill the blockchain economy before it even got off the ground. **In other words, if you believe in the future of blockchain apps, not only should you believe that a price-stable coin will be needed for interchange—you better hope that a price-stable coin will succeed.**

Fighting Macroeconomic Depressions

Imagine a world in which crypto has won over fiat. All savings are held in Bitcoin, and everything is priced and paid for in BTC—from groceries to gas, from new cars to new homes. What would happen if a Bitcoin lending service made a bunch of subprime loans that went bad, causing a repeat of the 2008 Great Recession?

Because there is no "Bitcoin Fed," there is a real risk the recession would balloon into a full-fledged macroeconomic depression. Many economists believe that the Fed's actions in the 2008 crisis helped save the world from another Great Depression. The high-level reasoning here is fairly simple: Imagine we're in a recession, and demand

for goods is falling. People buying fewer goods generally means that prices will fall. But when prices are falling, why make that home renovation for 10 BTC now, when it might only cost 5 BTC in a year? And so demand falls further, causing prices to continue to fall, and so on as part of a self-fulfilling prophecy. This phenomenon is known as a deflationary spiral, and it has been known to cause extraordinary losses in economic productivity, as happened during the Great Depression. One tool that central banks often use to fight these destructive spirals is an expansionary monetary policy that creates more money when price levels fall. However, any sort of dynamic monetary policy is impossible with existing cryptocurrencies because their money supply is fixed. On the other hand, the Basis protocol has a dynamic monetary policy built-in, and as a result, might be thought of as putting some of the core features of a central bank on the blockchain.

Cryptocurrency technology is rapidly advancing to the point where it will better serve citizens of hyperinflating economies than their local currencies, where it will serve as a more convenient stable asset for cryptocurrency traders than cash, and where it will enable cryptocurrency capital markets and a full blockchain economy to form. In this future world, governments would do well to support cryptocurrencies that are stable in the face of macroeconomic upheaval. In fact, citizens may even demand it.

How Basis Implements Price Stability

Basis implements price stability using the same economic principles relied upon by central banks around the world. The most important of these is the Quantity Theory of Money. In this section, we discuss the following topics:

- How the Quantity Theory of Money ties long-run price levels to the supply and demand for money.
- How the Basis protocol estimates changes in demand by monitoring the exchange rate between Basis and its pegged assets.
- How the Basis protocol expands and contracts Basis token supply based on the exchange rate.
- How these protocol-enforced actions incentivize speculators to make markets on Basis's exchange rate, maintaining Basis's peg even in the short-run.

The Quantity Theory of Money

History has shown that as markets rise and fall, people's choices in an economy are vulnerable to frenzies and panics. During an economic boom, people have more money, so they want to buy more goods, causing the prices of goods to rise, which fuels demands for higher wages, which means people have even more money. This is an inflationary spiral, and it happened to Germany in the 1920s, Brazil in the 1980s, and Argentina in the 1990s. Similarly, in an economic bust, people are afraid to buy goods, causing the prices of goods to drop, driving people to put off purchases further until prices fall even more, and so on. This is known as a deflationary spiral—and it almost occurred during the global recession of 2008. In both of these situations, a responsible central bank can step in to cut off these destructive feedback loops. But how do central banks manage this task?

Imagine that prices in an economy are at some level—say, the average cost of a predefined "basket of goods" is $100. The Quantity Theory of Money says that if you doubled the amount of money that everyone had in their bank accounts, then, in the long run, that same basket of goods would cost $200. Why? While the nominal amount of money everyone has has doubled, the true value of goods has stayed the same. This means that people should be willing to part with twice as much nominal money to get the same amount of value. The same principle applies in the reverse: If we yanked half of peoples' savings out of the economy, then in the long run, our same basket of goods would cost only $50.

Extending this concept, we consider the case of a central bank trying to calm inflation. High prices that are constantly rising mean that people are too willing to spend money. To restore prices, we could restrict people to have less money. (Let's put aside how for now.) Similarly, the opposite applies with deflation, which makes people unwilling to spend money. To restore prices, we could give people more money. This simple but important idea is exactly what central banks do to stabilize prices. While the tools that central banks use to implement monetary policy can be abstruse and difficult to understand, e.g., open market operations and reserve requirements, a central bank does two things at a high level:

- **Expand the money supply.** If a central bank sees that prices are going down, it can expand the money supply to bring them back up.
- **Contract the money supply.** If a central bank sees that prices are going up, it can contract the money supply to bring them back down.

Expanding and contracting the money supply works because the Quantity Theory of Money states that long-run prices in an economy are proportional to the total supply of money in circulation. Below is an example of the theory, applied to keep price levels

stable in a currency like Basis:

- Suppose you want to peg a currency like Basis such that 1 token always trades for 1 USD. We'll show that you can do this by growing or shrinking the supply of tokens in proportion with how far the current exchange rate is from the desired peg.
- First, we introduce the concept of *aggregate demand*. Conceptually, aggregate demand describes how much people in aggregate want the coin:
  demand = (coin price) * (number of coins in circulation)
  This is also known as a coin's market cap, since market cap equivalently describes how much people in aggregate value the coin.
- Let X represent the number of coins in circulation, i.e., coin supply. Suppose that demand has risen over the past few months such that coins are now trading for $1.10:
  demand = $1.10 * X
- To determine how coin supply can be adjusted to restore the peg of $1, assume that demand stays constant, and let Y represent the desired number of coins in circulation:
  demand_before = $1.10 * X
  demand_after = $1.00 * Y
  demand_before = demand_after
- Solving for Y implies that in order to get your coin to trade at $1, you need to increase the supply of your coin by a factor of 1.1:
  $Y = X * 1.1$

As a rough estimate, the Quantity Theory of Money finds that if Basis is trading at some price P that is too high or too low, the protocol can restore long-term prices to $1 by multiplying existing supply by P. There are some technical details that we'll get to later about how fast the protocol must respond, how fast prices will respond, and so on—but the core idea is that to maintain a peg in the long term, we just need to measure the price of Basis and adjust Basis supply accordingly.

The Basis Protocol

We have found that Basis will maintain its peg in the long run if token supply is adjusted to match token price. How does the Basis protocol measure token price? How does it adjust supply?

We tackle these questions here by providing a full specification of the Basis protocol. At a high level, the protocol can be understood as having all the technical properties

of a traditional cryptocurrency like Bitcoin, but with these additional features:

- **The protocol defines a target asset to stabilize against.** This might be the USD, another fiat currency, an index like the Consumer Price Index (CPI), or a basket of goods—let's use the USD as an example in the rest of this section. Then, the protocol defines a target price for Basis in the pegged asset—say, $1 for 1 Basis token.
- **The blockchain monitors exchange rates to measure price.** The blockchain sources a feed of the Basis-USD exchange rate via an oracle system. This can be done in a decentralized way, as we'll detail later.
- **The blockchain expands and contracts the supply of Basis tokens in response to deviations of the exchange rate from the peg.**
    - If Basis is trading for more than $1, the blockchain creates and distributes new Basis. These Basis are given by protocol-determined priority to holders of bond tokens and Base Shares, two separate classes of tokens that we'll detail later.
    - If Basis is trading for less than $1, the blockchain creates and sells bond tokens in an open auction to take coins out of circulation. Bond tokens cost less than 1 Basis, and they have the potential to be redeemed for exactly 1 Basis when Basis is created to expand supply. This incentivizes speculators to participate in bond sales and thereby destroy Basis in exchange for the potential that bond tokens will pay out in the future.

The Basis protocol might be better understood by comparing it with the Fed. Like the Fed, the Basis blockchain monitors price levels and adjusts the money supply by executing open market operations, which in our case consists of creating Basis or bond tokens. Like for the Fed, these operations are predicted by the Quantity Theory of Money to produce long-run price levels at the desired peg.

We now fill in the details of the protocol below.

Measuring the Exchange Rate

First, we explain how the Basis blockchain obtains the Basis-USD exchange rate. Since this information is external to the blockchain, the Basis protocol must implement what is known as an oracle system, i.e., a system that uploads outside information to a blockchain. This can be implemented in several ways:

- **Trusted feed.** The simplest approach is to have a single feed that uploads the real-world exchange rate to the blockchain, say from Coinbase, Kraken, or

another large exchange. This is obviously a point of centralization, but it bears mentioning nonetheless.

- **Delegated decentralized feed.** A semi-decentralized approach is to select a small group of feed uploaders by vote from holders of Basis. Given this set of feed uploaders, the system can choose the median exchange rate from them at fixed intervals. If any bad actor is consistently identified as trying to corrupt the feed, they can be voted out of the system by coin-holders who have an incentive to preserve the system's long-term value. This captures most of the benefits of decentralization. A similar scheme called Delegated Proof of Stake (DPoS) is even used in other protocols to generate entire blocks.
- **Decentralized Schelling point scheme.** A fully decentralized approach is to use a Schelling point scheme to determine the exchange rate. A Schelling point scheme operates something like this:
  - Anyone on the network can vote on what they think the average exchange rate was in the last 5 minutes.
  - Every 5 minutes, the votes are aggregated and weighted by the number of coins possessed by each voter. In other words, the more coins you have, the more weight your vote gets.
  - The weighted median is taken as the true exchange rate. Additionally, the weighted 25th and 75th percentiles of price estimates are computed.
  - People who guessed between the 25th and 75th percentiles are rewarded with a preset amount of newly-created Basis. This reward encourages people to vote, and furthermore to vote with the consensus.
  - Optionally, people who guessed outside the 25th or 75th percentiles can be penalized by having some of their stake slashed.

By weighting according to coin ownership, selecting the median, and including a consensus reward mechanism, the scheme largely protects itself from bad actors so long as no actor owns more than 50% of the voting coinbase. It will be necessary to design the scheme's reward and penalty rules so that enough people are incentivized to vote. Should these incentives be designed correctly, the result provides the same level of security as that offered by Bitcoin (which is similarly vulnerable if a single miner claims more than 50% of mining CPU), Ethereum (should it implement proof of stake), etc.

The trusted feed and delegated decentralized feed approaches are easy ways to securely bootstrap the protocol, with some sacrifices to decentralization. The Schelling point scheme is more novel, but we believe we can make it robust by properly engineering its incentives. Either way, all of these implementations are valid alternatives for providing the Basis blockchain with a feed of Basis-USD prices.

Expansion and Contraction via a Three-Token System

To expand and contract the supply of Basis, the Basis protocol defines three classes of tokens. We briefly mentioned these three classes earlier. Here, we define them explicitly:

- **Basis.** These are the core tokens of the system. They are pegged to the USD and are intended to be used as a medium of exchange. Their supply is expanded and contracted in order to maintain the peg.
- **Bond tokens.** Called bonds for short, these tokens are auctioned off by the blockchain when it needs to contract Basis supply. Bonds are not pegged to anything, and each bond promises the holder exactly 1 Basis at some point in the future under certain conditions. Since newly-created bonds are sold on open auction for prices of less than 1 Basis, you can expect to earn a competitive premium or "yield" for your bond purchase. The conditions under which a bond is redeemed are:
  - The blockchain is creating and distributing Basis, i.e., it has determined that an expansion of the Basis supply is necessary.
  - This bond has not expired, i.e., it has been fewer than 5 years since the bond was created.
  - All bond tokens that were created before this bond have been redeemed or expired.
- **Share tokens.** Called shares for short, these are tokens whose supply is fixed at the genesis of the blockchain. They are not pegged to anything, and their value stems from their dividend policy. When demand for Basis goes up and the blockchain creates new Basis to match demand, shareholders receive these newly-created Basiss pro rata so long as all outstanding bond tokens have been redeemed.

Expansion

Expansion works as follows. First, the blockchain tallies any outstanding bond tokens and orders them according to when they were created, with the oldest first. We call this ordered sequence of bonds the Bond Queue. The blockchain also tallies all outstanding share tokens. Then, the blockchain creates N new Basis tokens and distributes them as follows:

- **Bondholders are paid first, and in first-in-first-out (FIFO) order.** If there are any outstanding bond tokens, the blockchain begins converting bonds into coins, one-for-one, according to their order in the Bond Queue. For example,

if we need to create 100 Basis, we convert the 100 oldest outstanding bonds into 100 new coins. The FIFO queue incentivizes people to buy bonds sooner than later, since bonds bought sooner are paid out before bonds bought later.

- **Shareholders are paid after bondholders.** If there are no more outstanding bond tokens, the system distributes any remaining new coins to shareholders, pro rata, as a dividend. For example, if we need to create 1 million Basis, and there are 0 outstanding bonds and 10 million outstanding shares, then each share receives 0.1 Basis.

To prevent a situation in which the Bond Queue grows so long that speculators no longer value new bonds at the end of the queue, we also give bonds an expiration. The longer the Bond Queue grows, the longer it takes for new bonds at the end of the queue to get paid out. This causes the price of new bonds to drop since speculators start demanding a higher return for the extra time and risk that they take on. But if the price of new bonds drops to 0, the system cannot contract supply anymore—a price of 0 means that nobody wants to exchange their Basis for bond tokens. To prevent this from happening, we forcibly "expire" all bonds that have been in the Bond Queue for more than 5 years, even if they have yet to be redeemed. We selected a 5-year bond expiration after rigorous simulation showed that this produced a robust system with sufficiently high bond prices even in the face of wild price swings. We save the details for later discussion.

Is there a cost to having an expiration? Certainly. Leaving bonds permanently unpaid after an expiration makes bonds generally riskier, which pushes overall bond prices down. But the key insight is that expiring bonds greatly increases bond prices during critical, hypothetical scenarios where system demand has been contracting for an extended period of time. For example, if Basis demand dropped sharply one year, and it didn't recover enough over the next 5 years to pay for all the bond tokens created in that first year, those early bond tokens will simply expire. These expirations shorten the Bond Queue, helping buttress new bond prices to be higher than they would have been otherwise. Stepping back, we can see that an expiration strikes a tradeoff that penalizes calmer times in favor of critical times, which increases system stability.

Conceptually, the Bond Queue is similar to the US national debt. Just like how the Basis system creates bond tokens that go into the Bond Queue until they are paid, the government offers Treasury bonds that add to the national debt until they are paid. When the national debt grows too large, faith in Treasury bonds drops, resulting in higher borrowing costs against the future that eventually manifest as future inflation, higher future taxes, or future default. By capping the size of the Bond Queue and automatically defaulting on bonds that are too old, Basis disallows this tax on future stability. Instead, its fixed bond expiration transparently taxes the

present. An expiration, in other words, strikes a transparent balance between higher borrowing costs now (in the form of lower bond prices when the Bond Queue is short), and lower borrowing costs when we really need it (in the form of higher bond prices when the Bond Queue would otherwise be too long).

In summary, the expansion mechanism can also be understood through the following example:

- Suppose there are 500 bonds in the Bond Queue, 200 of which were created more than 5 years ago. Additionally, suppose there are 1,000 shares in circulation.
- Suppose the system needs to create 1,000 new coins.
- The system expires the 200 oldest bonds, leaving 300 bonds in the queue. If the system needed to create fewer than 300 coins, it would only redeem the oldest bonds. However, the system needs to create 1,000 coins, so it redeems all 300 bonds.
- The system still needs to create 700 more coins. The system distributes these 700 coins evenly across the 1,000 shares. Each share receives 700 / 1,000 = 0.7 coins. If you hold 100 shares for example, you would receive 70 coins during this expansion, which you can then sell for USD.

Contraction

Contraction works as follows. In order to destroy Basis, we must properly incentivize holders of Basis to lock up their Basis in exchange for future payoff. We do this by having the blockchain create and sell bond tokens. As discussed earlier, bond tokens are sold on open auction for prices that are generally less than 1 Basis. In return, they promise a future payout of 1 Basis when the system is expanding and when there are no older outstanding bonds, so long as the bond has not expired due to it having not been redeemed for 5 years.

First, we discuss the open auction system. In order to sell bonds, the blockchain runs a continuous auction in which bidders specify a bid and bid size for new bond tokens. In other words, auction participants specify how much Basis they want to pay for each bond and how many bond tokens they want to buy at that price. For example, one can specify that they would like to purchase 100 bonds for 0.9 Basis per bond. When the blockchain decides to contract coin supply, it chooses the orders with the highest bids and converts the holders' coins into bonds until sufficient Basis has been destroyed. As an example:

- Suppose the system wants to sell 100 bonds.
- Suppose that there are three buy orders on the order book: One bid for 80

bonds at 0.8 Basis each, one bid for 80 bonds at 0.6 Basis each, and one bid for 80 bonds at 0.4 Basis each.
- The system will compute the clearing price, which is a single price at which all offered bonds would have been bought at. Here, the clearing price is 0.6 Basis.
- The system will fill the winning bids at the clearing price: The first user will receive 80 bonds in exchange for 80 * 0.6 = 48 coins, and the second user will receive 20 bonds in exchange for 20 * 0.6 = 12 coins.

The protocol sets an artificial floor for the price of bond tokens in order to ensure that it doesn't borrow too heavily against the future in order to contract supply now. We currently set this floor at 0.10 Basis per bond. We have simulated bond prices to show that, under a very wide range of models of Basis demand, this floor is essentially never hit. We save further discussion for a subsequent section.

A Few Technical Notes

We have now specified the core of the Basis protocol, which explains how the blockchain expands and contracts the supply of Basis to maintain its peg. Here, we address the most common question we hear: Does it work?

In particular, we address the following concerns:

- **Robustness:** Is the blockchain always able to contract supply when it needs to by selling bond tokens?
- **Price responsiveness:** Does the blockchain respond quickly enough to price fluctuations, given that it operates on discrete time steps?

Robustness

Another way of asking the first question is: Under what scenarios will the price of new bond tokens hit the artificial floor? To answer this question, we constructed multiple different models for bond price and multiple different models for Basis demand as measured by market cap. Then, we ran Monte Carlo simulations with different parameterizations of these models to estimate the probability of bond price hitting the artificial floor under a wide variety of assumptions.

To provide some concreteness, our approaches to modeling market cap included the following:

- Modeling coin market cap as a geometric brownian motion (GBM), a model commonly used in equity option pricing theory. We fit GBM parameters for

drift and sigma on the historical returns of a variety of assets and indices like Bitcoin, Ethereum, the S&P 500, US 10-Year Treasuries, and the US GDP. We also simulated market caps on a dense grid of (drift, sigma) values to determine how robustness varies with these core input parameters.
- Modeling coin market cap using block bootstrapping, a method for sampling dependent test statistics from non-stationary time series data. We sampled from the returns of the same assets and indices mentioned above.

With regard to bond pricing, our approaches involved the following:

- Using risk-neutral pricing, another hallmark of option pricing theory, in which we assumed a replicating portfolio to determine bond price under a GBM model.
- Using a time-tested Sharpe Ratio pricing method to determine a bond price that does not rely on GBM assumptions.

While the details are beyond the scope of this whitepaper, we will publish a thorough robustness analysis paper discussing this work before network launch.

Price Responsiveness

One might be concerned that the Basis protocol doesn't react to price drops or price increases in real time. In particular, the protocol quantizes its actions into discrete time steps, suggesting that if there is a shock to the system, the price might be too low or too high for a prolonged period of time before the protocol responds. How can we be assured that exchange rates will be quickly brought back to the peg?

The critical insight is that as long as traders expect Basis price to correct in the long-term, they are incentivized to trade in the short-term to restore a peg. For example, suppose a speculator sees that Basis price is too low. As long as he believes that Basis price will correct because of a future protocol action, he is incentivized to buy coins now, in anticipation of the protocol's actions, to capitalize on the current, temporary drop in prices. Similarly, if a speculator sees that Basis price is too high, then he might take a short position, which puts downward, peg-restoring pressure on Basis price. These incentives exist even in advance of any reaction from the protocol.

Speculators taking long and short positions like this can be thought of as liquidity providers that buffer spikes in Basis demand, creating flexibility around when the protocol must respond.. Thus, as long as there is sufficient liquidity, and as long as speculators trust the protocol to restore Basis supply before this liquidity is used up, we should expect only small deviations in coin price around any peg.

A Post-USD World

By pegging to a local currency, a cryptocurrency piggybacks on all the hard work that a central bank does to stabilize its currency's purchasing power. In other words, Basis's peg to the USD lets it effectively copy the Fed's work of stabilizing the USD. But what happens if Basis gains popularity over time, acquiring users, to the point that it is as popular as credit cards, cash, and the dollar itself?

Imagine that one day, Basis is so widely used as a medium of exchange that it actually starts to displace the USD in transaction volume. Were this to happen, Basis would present the world with both the technology and the opportunity to develop an independent, transparent, and potentially more stable monetary policy than anything that's ever been possible via central bank. What does this mean for the future?

Stabilizing to a CPI

If Basis were to command a significant share of the world's transaction volume, we can assume that some goods will begin to be sold at prices denominated first in Basis. In such a world, the Basis protocol could be updated to a peg that is independent of any local currency—for example, Basis could stabilize against the Basis-denominated prices of a basket of goods. This would be similar to how the Fed stabilizes against a consumer price index (CPI) to maintain the purchasing power of the dollar. If developers find that built-in inflation is beneficial to the economy or the system, the new peg could even incorporate a 2% inflation target, just as the Fed does.

We envision a number of potential benefits in this scheme. First, unlike the Fed, Basis would implement its monetary policy using a transparent, decentralized algorithm, with no direct human input. We acknowledge that a fully automated monetary policy has its dangers. However, we believe that because the Basis protocol presents, for the first time, the technology for a verifiable, fully automated monetary policy, we will see research in algorithmic monetary policy advance in lockstep as Basis usage grows.

Additionally, a Basis protocol stabilized to the CPI implements a monetary policy that is independent of any government. At a high level, we believe that governments provide two critical services to their citizens in maintaining control over the money supply: Verifiability and price stability. In terms of verifiability, a central government helps protect the users of a currency against counterfeiting. In terms of price stability, a central bank helps smooth macroeconomic demand and, in some cases, manage unemployment—this is the Fed's so-called dual mandate. With the advent of Bitcoin and its solution to the double-spend problem, the need for centralized verifiability has

waned. For the first time, Basis also eliminates the need for centralized price stability. However well-intentioned and well-insulated a central bank may be, governments with integrated central banks will always have the incentive to print money to escape fiscal debts. We imagine that should citizens choose this technology over local currency alternatives, an independent, transparent, cryptocurrency-based monetary policy could offer society a level of accountability like never before seen in history.

As a final aside: If Basis were to transition to a CPI peg, a critic might argue that it would only fulfill one of the two current mandates of the Fed. In particular, it would stabilize prices but ignore unemployment. But this shortcoming is actually addressable. Think about what it means for the Fed to stabilize employment levels. During an economic shock, companies' demand for labor declines, bringing about unemployment and a drop in output. Observing these effects, the Fed prints money and pumps it into the economy, expecting that the money will be used to reduce unemployment and restore growth. But the Basis protocol can create Basis in response to unemployment just like how the Fed does—Basis can simply incorporate some index of unemployment or growth into the exchange rate uploaded to its blockchain. With this slight modification, we believe that Basis could replicate the Fed's dual mandate while maintaining full, transparent, protocol-enforced decentralization.

A Regional Basis for Each Regional Economy

While it might seem attractive to have a single global currency, the reality is that regional economies often benefit from having their own currencies that can respond independently to local demand shocks. This is because demand shocks can concentrate in a particular region, in isolation from the rest of the world. For example, this situation has recently caused problems for the Eurozone—Greece could see a massive drop in domestic demand that isn't shared by Germany. If Greece and Germany are using a single currency when this happens, they are no better off than if they were each using their own fixed-supply currencies. For this reason, in the long run, it may be favorable to create a separate instance of Basis for each regional economy, with each stabilizing against a CPI computed for that particular region. This would make the world's currency market similar to what we have today, only with each economy benefiting from the accountability and transparency of a codified monetary policy.

Other Attempts at a Stable Coin

We believe it's important to understand what others have tried in the past and are trying now. Below, we enumerate several stable coin attempts that we're aware of. We describe how they work and why we think they fall short of being robust.

Seigniorage Shares

Seigniorage Shares is a paper written in late 2014, and last updated in April 2015, that introduces the idea of expanding and contracting coin supply to maintain a peg. The system's philosophy of adjusting coin supply to match coin demand mirrors that used by central banks around the world. We also find some inspiration in it. However, we think there are a number of difficulties in this system's particular implementation.

In the Seigniorage Shares system, when coin price drops, "shares" are auctioned off for coins, destroying coins in the process. When coin price rises, coins are auctioned off for shares, creating coins in the process. Here are some of our biggest concerns about this approach:

- **It's hard to price a Seigniorage Share.** Since the Seigniorage Shares system maintains a peg by auctioning coins for shares and shares for coins, it is very important that investors feel comfortable pricing shares. While we believe the paper's method of pricing shares is theoretically correct, it seems fragile in practice. This point is a bit technically involved, but the paper asserts that if share owners always participate pro-rata in all auctions used to adjust coin supply, then they can always maintain their percentage ownership of shares outstanding. Since the aggregate payout for all Seigniorage Shares is just the sum of all future changes in coin supply, this means that a share can be priced as its current percentage of coins outstanding times the net present value of this aggregate payout. Even if a share owner does not participate in an auction used to adjust coin supply, the auction should adjust the value of her shares by her cost or payout had she participated in the auction. But the problem comes when auctions are not liquid enough. An illiquid auction could cause shares to trade at a lower price than predicted, and if a share owner skips the auction, she would be diluted far more than expected. This massive dilution would then hurt her perpetually. In other words, an illiquid auction at any time could dramatically hurt existing shareholders who don't participate in the auction. This is in contrast to the situation for most financial contracts, where an illiquid auction only hurts existing holders who *do* participate in the auction. Ideally,

a protocol's primary method of responding to dips in coin demand should not have a payout that is so dependent on future liquidity. In the Basis protocol, the payout of a bond token depends only on the queue of previously created bonds and the pattern of future expansions. Additionally, if one is ever worried about future liquidity, it is also much easier to set a price floor on Basis bonds than on Seigniorage Shares because a Basis bond's payout is always 0 or 1 coins.

- **No recovery from death spirals.** When coin demand drops, the Seigniorage Shares system creates more and more shares, causing share price to fall. Share price can be restored only if coin demand is restored; the protocol does nothing to encourage recovery from death spirals. On the other hand, Basis's bond expiration allows contraction to kick in again even after bond prices hit zero. With our protocol, if the Basis system creates a lot of bonds but demand doesn't recover, those bonds will eventually expire, restoring some contractionary capacity without requiring coin demand to fully restore again.
- **Death spirals are far more likely here than in Basis.** When coin demand drops, there is no incentive for people to buy shares early in the drop rather than later in the drop, since shares bought earlier pay off the same as shares bought later. This means that if people suspect an upcoming drop in coin demand, share price will immediately crash. It is thus easier in the Seigniorage Shares system for there to be a panic for panic's sake, since if share price ever hits 0, the system can no longer contract, and everyone will want to get their money out of the system before that happens. On the other hand, Basis's first-in-first-out bond queue means that bonds bought early pay out early. Thus, in the Basis system, people are incentivized to buy bonds as soon as the dip starts. This instant incentive to buy bonds reduces the likelihood of death spirals.

MakerDAO

MakerDAO is a project that aims to create a stable token, called Dai, backed by decentralized reserves. At a small scale, we think it is relatively easy for any system to remain stable by having early supporters subsidize a stable price for the coin. But we think Dai does not sufficiently balance supply and demand to stay stable in the long-term.Examining the incentives behind the MakerDAO protocol, we've come to believe that:

- **Dai is unscalable.** Dai supply is restricted because there is insufficient incentive for people to lock up collateral in CDPs. CDPs offer collateral holders the opportunity to obtain leverage in a decentralized way. However, the MakerDAO system requires that CDP owners borrow in Dai. Since Dai can spike up in value

during collateral crashes, when someone locks up collateral in a CDP, they must either lock up their collateral at a very high collateral-to-debt ratio resulting in low amounts of leverage, or they must bear the risk of having to repurchase Dai at a higher price to close their CDP and avoid liquidation. Neither makes CDPs very competitive with other alternatives for leverage, since centralized futures and other upcoming decentralized lending services arguably offer less risk, more leverage, and a better user experience.

- **Dai price can easily float up to the liquidation ratio (~$1.50 for example).** Aside from the belief that Dai is worth $1, there is no incentive that keeps Dai from wandering up to a higher price. To see this, imagine that there is a collateral crash, say in ETH. On the one hand, people are fleeing ETH and flocking to more stable assets, increasing the demand for Dai. On the other hand, the collateral-to-debt ratio of CDPs is falling, causing Dai to be destroyed as some CDPs are liquidated while some others are closed by their owners to avoid liquidation. The combination of Dai demand increasing just as Dai supply decreases causes Dai price to spike above $1, restricting the usefulness of Dai just as people need it. In these situations, only early supporters who hold large amounts of ETH can be relied upon to subsidize the creation of more Dai by locking up more ETH in CDPs. Absent this artificial force, Dai price is free to rise as high as demand takes it, potentially up until the liquidation ratio, at which point CDPs are allowed to hold less ETH than the a Dai is worth, creating a riskless arbitrage. Note that this assumes the system's Target Rate Feedback Mechanism is disabled.
- **Dai is fundamentally unstable with its Target Rate Feedback Mechanism enabled.** This mechanism aims to stabilize the price of Dai by adjusting the rate at which Dai's target price changes. While this creates an incentive for Dai to revert to its target price, it also changes where that target price moves. When triggered, Dai is more stable, but it is "stabilized" against an unstable, unpredictable target.
- **Dai and MKR devalue under massive crashes in collateral.** In the worst of collateral crashes, MakerDAO's auto-liquidation policy means that either Dai devalues or MKR devalues, and there is no mechanism for restoring prices.
- **MKR, the investor token for MakerDAO, pays out poorly.** It earns very little from stability fees, and it is subject to the risk of occasional dilution.
- **The MakerDAO stability analysis totally fails to analyze the protocol's economic incentives.**

From a high level, we find the idea of a reserve-backed cryptocurrency intrinsically appealing. If a reserve-based system can create a rewarding enough incentive for people to deposit reserves, and it can additionally address counterparty risk and the

risk of its reserves suffering a black swan crash, then it should be able to remain broadly stable, at least in the short to medium term. However, we think it's very difficult for a project to overcome all of these hurdles.

We think that MakerDAO can grow to a small size, subsidized by its early supporters on the supply side and serving fans of decentralized reserve-based currencies on the demand side. However, because MakerDAO doesn't solve the fundamental challenges of building a reserve-backed cryptocurrency, MakerDAO ends up neither widely usable, nor particularly stable.

Tether

Tether is very interesting, but to us it's not really a cryptocurrency. Tether is run by a company that stores one USD in its reserves for every Tether coin that it mints, and it promises its users the ability to retrieve their USD by returning the Tether coin that accounted for it. In other words, Tether is basically a company taking deposits and issuing their own currency, similar to what eGold was doing in the 1990s—in fact, there is no reason Tether even needs to be a cryptocurrency, rather than a centralized database. While this centralized reserve-based approach can work in the short run, we think there are significant disadvantages overall:

- There is a risk that any company taking fiat reserves will be shut down at any time, just like what happened with eGold. The Tether team has been secretive about its banking relationships and restrictive when users want to withdraw their USD.
- The owners of Tether have complete control over the money supply, which makes them a single point of failure in general.
- Tether can never become independent from fiat because its value fundamentally comes from fiat. In contrast, Basis has a monetary policy built-in, providing for a smooth transition off of a fiat peg and to a consumer price index in the long run.

BitShares

Below is how BitShares stable coins work.

- There are BitShares and BitUSD, a multi-asset system like Basis.
- BitShares implements an exchange on its blockchain between the two, so there are always people willing to buy/sell both assets.

- People can do two things: They can "go long" BitUSD, which means they make money when it goes up, or they can "go short" BitUSD, which means they make money when it goes down.
- If you want to long BitUSD, you just buy a BitUSD for its listed price with dollars. That part's easy. Then, if the price goes up, you can sell it for its listed price later and make money.
- If you want to short BitUSD, you give the blockchain $1 in BitShares, as determined by the exchange rate feed, and it'll lock it up for 30 days. Then, there are a few nuances to what happens:
  - If the price of BitUSD goes up, then you'll get *fewer* BitShares back after 30 days.
  - If the price of BitUSD goes up *a lot*, you might get margin-called and lose all of your BitShares.
  - If the price of BitUSD goes down, then you'll get *more* BitShares.

  Under the hood, when you put your $1 worth of BitShares onto the blockchain, the blockchain does the following:
  - It creates 1 BitUSD out of thin air.
  - It sells that BitUSD to someone, thus effectively increasing the supply of BitUSD.
  - This is also how shorting works in real life, but you don't have to worry about it as a shorter—you just give it your BitShare and then you get back more/less depending on what happens to the price of BitUSD.
- BitUSD only exists because someone decided to enter a short contract. If nobody wanted to short BitUSD using BitShares, then no BitUSD would exist.
- When you sell a BitUSD you can either give it to someone else, or you can autoliquidate the person who has the other side of a short contract. If you do the latter, the supply of BitShares increases, driving up the price of BitUSD.

Overall, the BitShares protocol has several drawbacks that are deal-breakers for implementing a stable coin:

- **The BitUSD peg is enforced by a weak self-reinforcement scheme backed by the BitShares company as a lender of last resort, not by the protocol itself.** The only reason BitShares are worth 1 USD is because everyone believes it'll be worth 1 USD, and therefore everyone always shorts and longs in order to keep it there. If everyone one day just decides that BitUSD should be worth $100, then the equilibrium will adjust, and it'll re-peg to $100. The only reason it's even stayed stable this long is likely because the BitShares company acts as lender of last resort to enforce the peg when someone tries to break it. But this will almost certainly get too expensive one day, resulting in the complete breakdown of BitUSD as a price-stable currency. Incidentally,

when we explained this to one of our friends, he immediately suggested we raise a few million dollars and use it to demolish the peg by bidding it up to a new equilibrium, which would be extremely profitable, in the same way George Soros broke the bank of England. Note that this is much different from Basis's protocol, where a negative feedback loop is enforced at a protocol-level to keep the price pegged to $1.

- **BitShares wasn't designed to be a stable coin, it was designed to be a prediction market.** Although the above weakness is a complete deal-breaker for a stable coin in our opinion, it's important to remember that BitShares is useful for much more than a stable coin—it's a generalized prediction market that you can use to place bets on anything. For that reason, we would guess (though we don't know for sure) that BitShares wasn't even really designed to implement a stable coin, and the fact that you can have them on its platform is just a happy coincidence, and a testament to how generalizable their platform is.

Conclusion

Imagine a world in which Bitcoin starts competing with the USD in transaction usage. You would get paid in Bitcoin but pay rent in USD, or perhaps vice versa. This just doesn't make sense given Bitcoin's inherent volatility.

In this paper, we introduced Basis, a robust, decentralized implementation of a price-stable cryptocurrency. We believe that if we can just make it so that purchasing power doesn't fluctuate, people will shift from a mindset in which they hold as little cryptocurrency as possible, to a mindset in which they are comfortable holding their savings or revenue in it. We believe this contribution will trigger cryptocurrencies to undergo a virtuous cycle of adoption and help them transition into a mainstream medium of exchange—a result that has eluded every other cryptocurrency thus far.

Contact

If you have any thoughts or want to be involved in the project, feel free to email the authors as shown on the title page. For the most up-to-date version of this whitepaper, please visit http://www.basis.io.